



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1800
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/730,773	12/09/2003	Akashi Satoh	JP920020207US1	4832
48813	7590	07/06/2007		
LAW OFFICE OF IDO TUCHMAN (YOR)			EXAMINER	
82-70 BEVERLY ROAD			DADA, BEEMNET W	
KEW GARDENS, NY 11415				
			ART UNIT	PAPER NUMBER
			2135	
			MAIL DATE	DELIVERY MODE
			07/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/730,773

Applicant(s)

SATO ET AL.

Examiner

Beemnet W. Dada

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 09 December 2003.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-23 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-23 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 09 December 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date See Continuation Sheet.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :11/22/04, 1/30/06, 04/20/06, 10/17/06.

DETAILED ACTION

1. Claims 1-23 have been examined.

Claim Objections

3. Claim 13 is objected to because of the following informalities: claim 13 recites an verification encryption key at line 8, that should be changed to a verification encryption key. Appropriate correction is required.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 1-6, 13-16, 22 and 23 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

6. Claims 1, 5, 13, 22 and 23 are directed to data encryption and user verification. The examiner respectfully asserts that the claimed subject matter does not fall within the statutory classes listed in 35 USC 101. Claims 1, 5, 13, 22 and 23 are directed to functional descriptive material (i.e., software, see specification page 43, line 16 - page 44, line 8). Claims 1, 5, 13, 22 and 23 are rejected as being directed to functional descriptive material (i.e., computer software). Claims 2-4, 6 and 14-16 depend from claims 1, 5 and 13 and are rejected under the same rationale.

Claim Rejections - 35 USC § 102

Art Unit: 2135

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 7-9 are rejected under 35 U.S.C. 102(b) as being anticipated by Jackson EP 0 911 738 A2.

9. As per claim 7, Jackson teaches a hard disk device comprising:

a magnetic disk being a recording medium (i.e., mass storage device, such as floppy disks, magnetic taps) [column 5, lines 5-12];

a read-and-write mechanism for writing and reading data in and out of the magnetic disk [column 5, lines 12-15]; and

a control mechanism having an encryption function for encrypting data to be written in the magnetic disk and for decrypting the encrypted data to be read out of the magnetic disk (i.e., encryption/decryption of data to and from the disk) [column 5, lines 15-19], the control mechanism for controlling reading and writing the data by the reading-and-writing mechanism [column 5, lines 12-15], wherein the control mechanism executes encryption of the data to be written in the magnetic disk for each unit of writing and reading data in and out of a storage area of the magnetic disk upon processing of writing the data in the magnetic disk [column 11, paragraphs 0041 & 0042], in response to turning on and off of the encryption mechanism (i.e., activating the encryption/decryption only in response to receipt of a valid password) [column 5, lines 19-34].

Art Unit: 2135

10. As per claim 8, Jackson further teaches the device wherein the control mechanism judges as to whether the data are encrypted or not upon reading the data out of the storage medium, and further decrypts the data when the data are encrypted [page 11, paragraphs 0041-0042].

11. As per claim 9, Jackson further teaches the device wherein the control mechanism decrypts the read-out data when the data read out of the recording medium are encrypted, and the control mechanism encrypts and writes the data in the recording medium when the encryption function is turned on [page 11, paragraphs 0041-0042].

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

13. Claims 1, 2, 5, 6 and 13-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsuzaki et al. US 2001/0056541 A1 (hereinafter Matsuzaki) in view of Johnson et al. US 5,604,800 (hereinafter Johnson).

14. As per claim 1, Matsuzaki teaches a data storage device for an information processing device, the data storage device comprising:

an encryption circuit (i.e., encryption units E1-E4) for encrypting desired data (i.e., encrypting file key using read key) and personal identification information by use of an encryption key (i.e., encrypting password using read key) [paragraphs 0141 and 0152];

a recording medium for recording the data and the personal identification information encrypted by the encryption circuit (i.e., writing the encrypted password and encrypted file key as a file) [paragraphs 0141 and 0152]; and

a control unit for executing user verification by use of the encrypted personal identification information stored in the recording medium (i.e., the encrypted password is decrypted and used as an encryption key to encrypt a file key) [paragraphs 0145 & 0150], further the user inputs the password for decrypting the encrypted file key [paragraphs 0156-0159]). Matsuzaki is silent on the device wherein the encryption key is created out of a given piece of the personal identification information. However, such feature is old and well known in the art, which has an advantage of enhancing security of the system. For example, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of Matsuzaki in order to enhance the security of the system.

15. As per claim 5, Matsuzaki teaches a data storage device for an information processing device, the data storage device comprising:

an encryption circuit for encrypting desired data by use of a first encryption key (i.e., encrypting plaintext file using file key) and for encrypting the first encryption key (i.e., encrypting file key using read key) and personal identification information by use of a second encryption key (i.e., encrypting password using read key) [paragraphs 0141, 0147, 0148 and 0152]

a recording medium for recording the data encrypted by use of the first encryption key, the first encryption key encrypted by use of the second encryption key, and the personal identification information encrypted by use of the second key (i.e., writing the encrypted data, encrypted password and encrypted file key as a file) [paragraphs 0141, 0148 and 0152]; and

a control unit for executing user verification by use of the encrypted personal identification information stored in the recording medium (i.e., the encrypted password is decrypted and used as an encryption key to encrypt a file key) [paragraphs 0145 & 0150], further the user inputs the password for decrypting the encrypted file key [paragraphs 0156-0159]). Matsuzaki is silent on the device wherein the encryption key is created out of a given piece of the personal identification information. However, such feature is old and well known in the art, which has an advantage of enhancing security of the system. For example, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of Matsuzaki in order to enhance the security of the system.

16. As per claims 13 and 14, Matsuzaki teaches an information processing device comprising:

an operation control unit for executing various operation processing [figure 10, File management apparatus]; and

a data storage device for storing data to be processed by the operation control unit [figure 10, File management apparatus],

wherein the data storage device includes an encryption function for encrypting desired data by use of a data encryption key (i.e., encrypting plaintext file using file key) and for

Art Unit: 2135

encrypting personal identification information by use of an verification encryption key (i.e., encrypting password using read key) [paragraphs 0141 and 0152], and

the data storage device executes user verification by use of the encrypted personal identification information (i.e., the encrypted password is decrypted and used as an encryption key to encrypt a file key) [paragraphs 0145 & 0150], further the user inputs the password for decrypting the encrypted file key [paragraphs 0156-0159]). Matsuzaki is silent on the device wherein the verification encryption key is created out of a given piece of the personal identification information. However, such feature is old and well known in the art, which has an advantage of enhancing security of the system. For example, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of Matsuzaki in order to enhance the security of the system.

17. As per claims 17 and 22, Matsuzaki teaches a data processing method for a data storage device for executing data writing and reading in and out of a recording medium of a data storage device, the data processing method for a data storage device comprising the steps of:

encrypting personal identification information by use of an encryption key and thereby recording the encrypted personal identification information in the recording medium as verification data (i.e., encrypting password using read key and storing the encrypted password) [paragraphs 0141 and 0152];

executing user verification based on the verification data recorded in the recording medium(i.e., the encrypted password is decrypted and used as an encryption key to encrypt a

file key) [paragraphs 0145 & 0150], further the user inputs the password for decrypting the encrypted file key [paragraphs 0156-0159]); and

executing any of encrypting write data transmitted from a host system by use of the encryption key and thereby recording the encrypted write data in the recording medium (i.e., encrypting file key by using read key) [paragraph 0152], and, decrypting the data read out of the recording medium by use of the encryption key and thereby transmitting the decrypted data to the host system (i.e., decrypting the encrypted file key using the read key) [paragraph 0161]. Matsuzaki is silent on the device wherein the encryption key is created out of a given piece of the personal identification information. However, such feature is old and well known in the art, which has an advantage of enhancing security of the system. For example, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of Matsuzaki in order to enhance the security of the system.

18. As per claims 19 and 23, Matsuzaki teaches a data processing method for a data storage device for executing data writing and reading in and out of a recording medium of a data storage device, the data processing method for a data storage device comprising the steps of:

encrypting a personal identification information by use of a verification encryption key and recording the encrypted personal identification information in the recording medium as verification data (i.e., encrypting password using read key and storing the encrypted password) [paragraphs 0141 and 0152], and further encrypting a data encryption key by use of the verification encryption key (i.e., encrypting file key using read key) and thereby recording the encrypted data encryption key in the recording medium [paragraphs 0141 and 0152];

executing user verification based on the verification data recorded in the recording medium (i.e., encrypting file key by using read key) [paragraph 0152], and, decrypting the data read out of the recording medium by use of the encryption key and thereby transmitting the decrypted data to the host system (i.e., decrypting the encrypted file key using the read key) [paragraph 0161];

decrypting the data encryption key recorded in the recording medium by use of the verification encryption key (i.e., decrypting file key using read key) [paragraph 0161]; and

executing any of encrypting write data transmitted from a host system by use of the decrypted data encryption key and thereby recording the encrypted write data in the recording medium (i.e., encrypting data using file key), and decrypting the data read out of the recording medium by use of the data encryption key (i.e., decrypting data using file key) and thereby transmitting the decrypted data to the host system [paragraphs 0147, 0148 and 0164].

Matsuzaki is silent on the device wherein the encryption key is created out of a given piece of the personal identification information. However, such feature is old and well known in the art, which has an advantage of enhancing security of the system. For example, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of Matsuzaki in order to enhance the security of the system.

19. As per claims 2, 15 and 16, Matsuzaki further teaches the device wherein the encryption circuit encrypts the encryption key by use of a different encryption key, and the recording medium records the encryption key encrypted by use of the different encryption key [paragraphs 0148- 0152].

20. As per claim 6, Matsuzaki further teaches the device wherein the encryption circuit decrypts the encrypted first encryption key being read out of the recording medium by use of the second encryption key, and executes any of encryption and decryption of the desired data by use of the decrypted first encryption key [paragraphs 0161-0164],

21. As per claim 18, Matsuzaki further teaches the device further comprising the steps of: encrypting the encryption key by use of a different encryption key and thereby recording the encrypted encryption key in the recording medium [paragraphs 0148-0152]; and

decrypting the encrypted encryption key by use of the different encryption key and thereby decrypting the data read out of the recording medium by use of the decrypted encryption key [paragraphs 0161-0164].

22. As per claim 20, Matsuzaki further teaches the device further comprising the step of: decrypting the encrypted data encryption key recorded in the recording medium along with a change in the personal identification information by use of the verification encryption key created out of the personal identification information prior to the change, and then encrypting the data encryption key again by use of the verification encryption key created out of the personal identification information after the change and thereby storing the data encryption key in the recording medium [paragraphs 0192-0199].

23. As per claim 21, Matsuzaki further teaches the device further comprising the step of: decrypting the encrypted data encryption key recorded in the recording medium upon disabling encryption of the data recorded in the recording medium by use of the verification encryption

Art Unit: 2135

key created out of the personal identification information prior to a change and thereby storing the decrypted data encryption key in the recording medium [paragraphs 0192-0199].

24. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Matsuzaki US 2001/0056541 A1 in view of Johnson US 5,604,800 and further in view of Hirota et al. US 7,062,652 B1 (hereinafter Hirota).

25. As per claim 3, the combination of Matsuzaki and Johnson teaches the claimed invention as described above. However, the combination of Matsuzaki and Johnson does not explicitly teach the device, wherein the recording medium includes a special storage area which is inaccessible in normal use, and the recording medium records the encryption key in the special storage area. In the same field of endeavor, Hirota teaches a recording medium includes a special storage area which is inaccessible in normal use, and the recording medium records the encryption key in the special storage area [see for example, column 12, lines 49-54 and column 10, lines 22-36]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Hirota within the combination of the Matsuzaki and Johnson thereby protecting access to secure data and further enhancing security of the system.

26. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Matsuzaki US 2001/0056541 A1 in view of Johnson US 5,604,800 and further in view of Jackson EP 0 911 738 A2

27. As per claim 4, the combination of Matsuzaki and Johnson teaches the claimed invention as indicated above. Furthermore, Matsuzaki teaches device wherein the encryption circuit encrypts the encryption key by use of a different encryption key, and the recording medium records the encryption key encrypted by use of the different encryption key [paragraphs 0148- 0152]. The combination of Matsuzaki and Johnson does not teach a recording medium that manages the storage areas in accordance with the plurality of keys, and records the encrypted data in the respective storage areas by use of the corresponding encryption keys. However, Jackson teaches a device wherein the encryption function of the control mechanism creates a plurality of encryption keys out of a plurality of personal identification information and controls the user identification and the data encryption depending on each of the plurality of encryption keys, and the magnetic disk manages storage areas in accordance with the plurality of keys, and records the encrypted data in the respective storage areas by use of the corresponding encryption keys [page 8, lines 33-47]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Jackson within the combination of Matsuzaki and Johnson in order to efficiently process encryption/decryption of data.

28. Claims 10-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jackson EP 0 911 738 A2 in view of Johnson et al. US 5,604,800 (hereinafter Johnson).

29. As per claims 10 and 12, Jackson further teaches the device wherein the control mechanism includes an encryption function for encrypting desired data by use of a first encryption key and for encrypting the first encryption key and personal identification information by use of a second encryption key [page 7, paragraph 0028 and page 8, lines 21-32] and the

Art Unit: 2135

control mechanism executes user verification by use of the encrypted personal identification information [page 8, lines 21-32]. Jackson is silent on the device wherein the encryption key is created out of a given piece of the personal identification information. However, such feature is old and well known in the art, which has an advantage of enhancing security of the system. For example, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of Jackson in order to enhance the security of the system.

30. As per claim 11, Jackson further teaches the device wherein the encryption function of the control mechanism creates a plurality of encryption keys out of a plurality of personal identification information and controls the user identification and the data encryption depending on each of the plurality of encryption keys, and the magnetic disk manages storage areas in accordance with the plurality of keys, and records the encrypted data in the respective storage areas by use of the corresponding encryption keys [page 8, lines 33-47].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

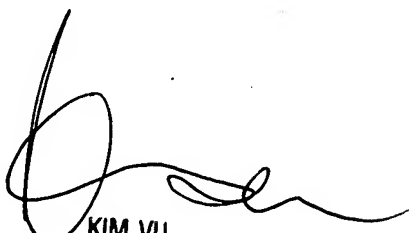
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Beemnet W Dada

April 15, 2007



KIM VU
PATENT EXAMINER
TECHNOLOGY CENTER 2100